



Les 5 éléments clés pour hiérarchiser la remédiation des vulnérabilités



Présentation

Les équipes IT sont débordées par l'abondance de vulnérabilités, de plus en plus nombreuses chaque jour. Le service informatique tente d'identifier les menaces les plus critiques qu'il devra gérer immédiatement pour protéger l'entreprise contre tout compromis.

Essayer d'éradiquer 100% des vulnérabilités de manière séquentielle, en leur accordant toutes la même importance, est une stratégie impraticable, irréaliste et dangereuse.

CERTAINES VULNÉRABILITÉS REPRÉSENTENT UN RISQUE MINEUR TANDIS QUE D'AUTRES DOIVENT ÊTRE RÉSOLUES IMMÉDIATEMENT

Ignorer les vulnérabilités sérieuses pendant trop longtemps tout en s'intéressant à celles secondaires c'est un peu comme décider de repeindre une maison dont le toit risque de s'effondrer... Qui plus est, le potentiel de dommage des vulnérabilités varie en permanence. Une vulnérabilité longtemps considérée comme insignifiante ou presque peut soudainement devenir plus critique si un kit d'exploit devient largement disponible.

Par conséquent, les entreprises qui ne parviennent pas à hiérarchiser correctement la remédiation des vulnérabilités courent le risque d'essuyer des cyberattaques dévastatrices. Elles encourent des dommages importants et durables pour leur fonctionnement, leur situation financière, l'image de la marque et la réputation de l'entreprise ainsi qu'au niveau des relations avec leurs clients et partenaires.

5 éléments clés pour hiérarchiser avec succès la remédiation des vulnérabilités

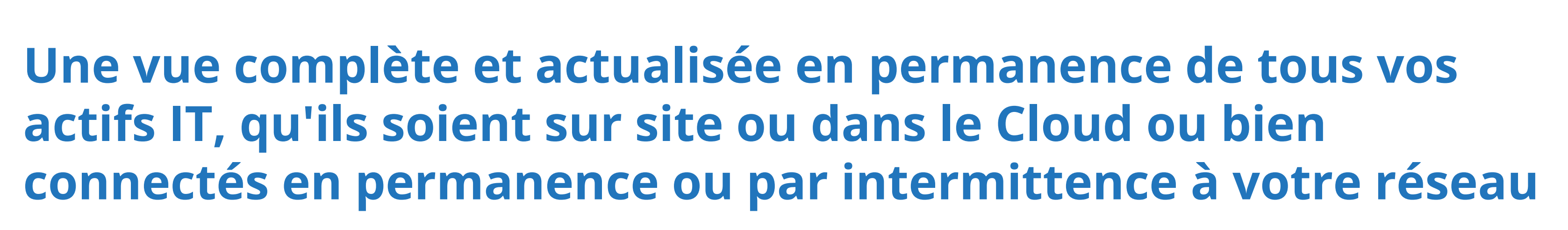
- ✔ Une vue complète et actualisée en permanence de tous vos actifs IT
- ✔ La connaissance du flux constant de divulgations des vulnérabilités
- ✔ La possibilité de corréler des informations sur les menaces externes avec vos vulnérabilités
- ✔ Des outils de tableau de bord pour visualiser votre paysage de menaces
- ✔ Des évaluations précises des scénarios de menaces pour votre entreprise



1

UNE VUE COMPLÈTE ET ACTUALISÉE EN PERMANENCE DE TOUS VOS ACTIFS IT





Une vue complète et actualisée en permanence de tous vos actifs IT, qu'ils soient sur site ou dans le Cloud ou bien connectés en permanence ou par intermittence à votre réseau

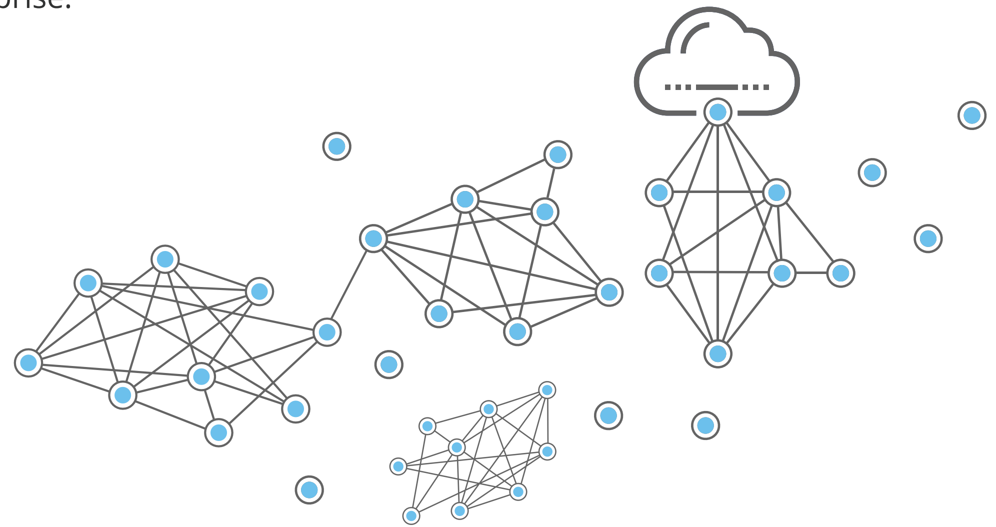
Lorsque vous tentez de hiérarchiser la remédiation des vulnérabilités, ce sont les éléments que vous ne connaissez pas qui entravent vos efforts. Cela implique d'avoir au départ la connaissance de tous les matériels et logiciels appartenant à votre entreprise, depuis les systèmes d'infrastructure jusqu'aux applications mobiles.

Il ne peut y avoir de serveurs, PC, smartphones, tablettes, imprimantes, applications ou middleware « fantômes » sur votre réseau sans que vous le sachiez. Vous devez avoir une vue complète et claire de votre environnement informatique à tout moment et être immédiatement au courant des changements opérés.

UN ACTIF IT INVISIBLE SUR LEQUEL IL EST IMPOSSIBLE D'ANALYSER LES VULNÉRABILITÉS EST UNE BOMBE À RETARDEMENT QUI ATTEND D'ÊTRE DÉCLENCHÉE PAR UN ATTAQUANT.

En plus de devoir disposer d'une liste complète de vos actifs IT, vous devez pouvoir accéder de manière granulaire et détaillé aux composants de chacun d'entre eux. Il vous faut également connaître le niveau d'interconnexion et de dépendance de chaque actif par rapport aux autres systèmes. Enfin, il est vital de savoir quel rôle joue chaque actif au sein de votre environnement IT global ainsi que sa valeur et son importance pour votre entreprise.

Cette connaissance contextuelle accompagnée de données détaillées est indispensable pour lancer le processus de hiérarchisation de la remédiation des vulnérabilités. En l'absence de cette structure informationnelle sous-jacente, vos tentatives d'évaluation des risques de vulnérabilités s'appuieront sur des informations inexactes et seront finalement une source d'erreurs et d'inefficacité.





2

LA CONNAISSANCE CONSTANTE DE DIVULGATIONS DES VULNÉRABILITÉS

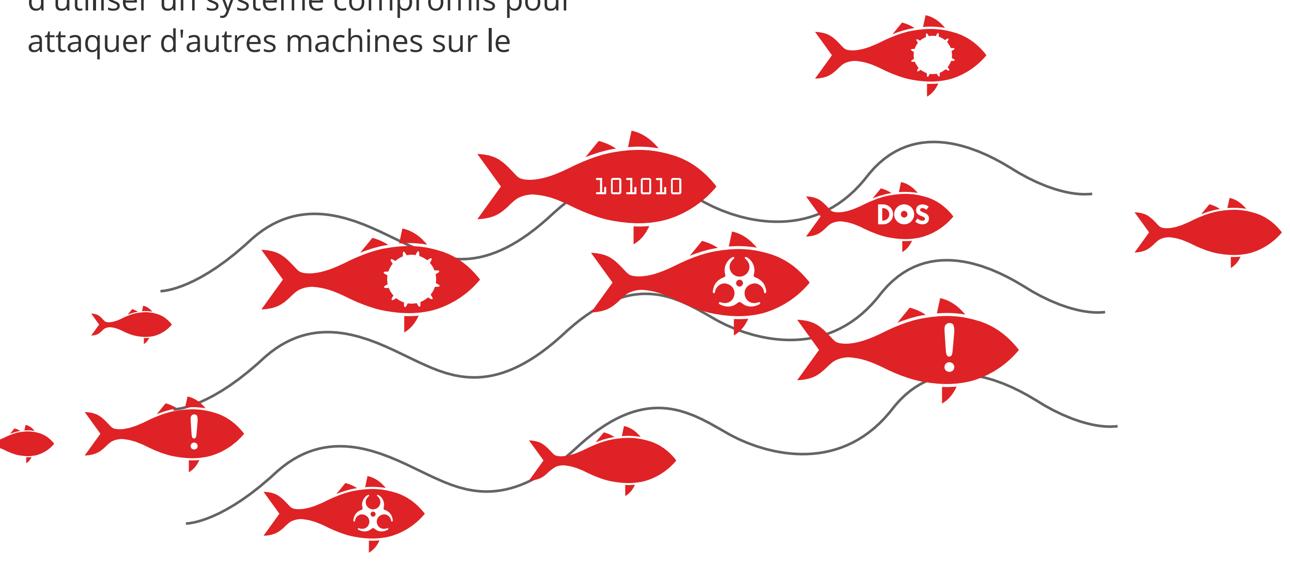


Connaissance constante de divulgations des vulnérabilités concernant la sécurité de l'information

Tout comme vous devez connaître de manière claire et approfondie tous les actifs IT de votre entreprise, **VOUS DEVEZ AUSSI VOUS INTÉRESSER AUX DIVULGATIONS DES VULNÉRABILITÉS EXTERNES POUR ÊTRE INFORMÉ DES TOUTES DERNIÈRES MENACES LANCÉES EN MODE AVEUGLE.**

Ces informations sur les divulgations proviennent d'un flux constant émis par de nombreuses sources, qu'il s'agisse d'acteurs du marché, d'administrations, de chercheurs universitaires, d'analystes technologiques ou encore de fournisseurs de solutions de sécurité.

Vous devez par exemple être conscient des vulnérabilités « Zero Day » activement exploitées, des codes d'exploitation publiquement disponibles, des vulnérabilités activement attaquées ; mais aussi des vulnérabilités par « mouvement latéral » permettant aux pirates d'utiliser un système compromis pour attaquer d'autres machines sur le même réseau, des vulnérabilités ayant un fort potentiel de perte de données, des attaques par déni de service distribué (DDoS) et des déclenchements de malware.







3

LA POSSIBILITÉ DE CORRÉLER DES INFORMATIONS SUR LES MENACES EXTERNES AVEC VOS VULNÉRABILITÉS



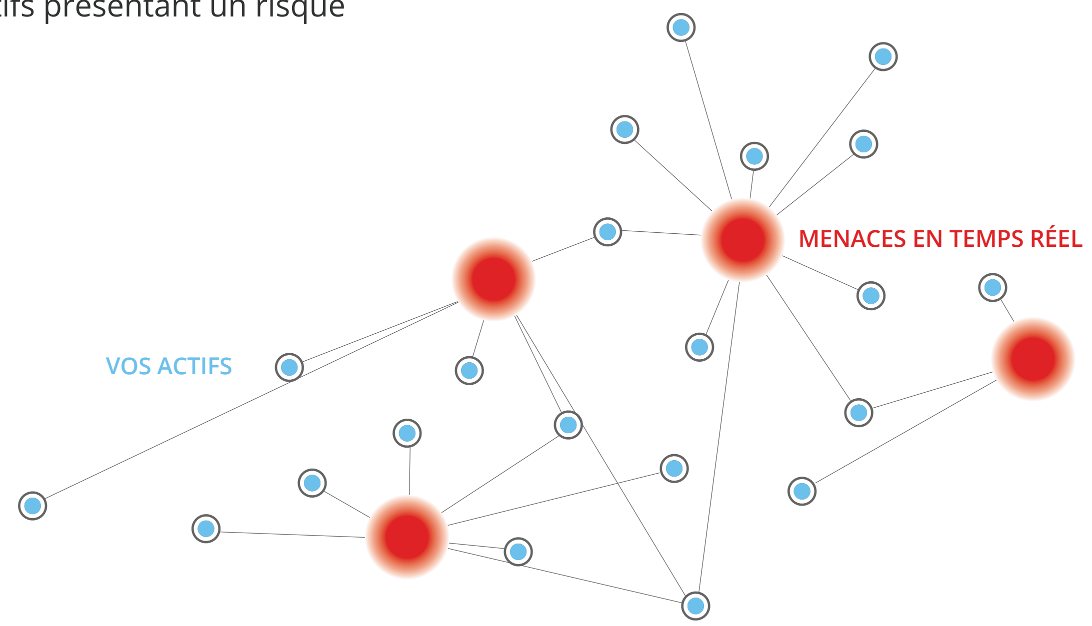
La possibilité de corréler des informations sur les menaces externes avec les vulnérabilités présentes dans votre environnement

Imaginons que vous ayez une vue à la fois complète et détaillée du paysage de vos actifs IT et que vous soyez parfaitement au courant des milliers de vulnérabilités qui sont divulguées. C'est bien, mais ce n'est pas suffisant. En effet, il vous faut maintenant faire des rapprochements, mais procéder manuellement est une tâche fastidieuse.

VOUS DEVEZ ASSOCIER LES DEUX ENSEMBLES DE DONNÉES INTERNES ET EXTERNES, À SAVOIR LES INFORMATIONS SUR VOS ACTIFS IT ET LES VULNÉRABILITÉS DIVULGUÉES, PUIS LES FAIRE CORRESPONDRE.

Il vous faudra le faire en permanence pour recevoir une alerte en cas de correspondance.

Vous devez également pouvoir effectuer des recherches spécifiques de manière proactive, en associant de nombreuses variables, pour trouver les actifs présentant un risque potentiel. Vous obtiendrez ainsi un instantané dynamique de toutes les vulnérabilités présentes dans votre environnement IT à un moment spécifique.





4

DES OUTILS DE TABLEAUX DE BORD POUR VISUALISER VOTRE PAYSAGE DE MENACES





Tableaux de bord, panneaux de contrôle, outils de création de graphes et de reporting pour visualiser votre paysage des menaces de manière holistique et consolidée

Après avoir corrélé vos données sur les menaces internes et externes et identifié les actifs IT impactés, vous devez pouvoir explorer les données, y rechercher des caractéristiques, les disséquer et les analyser puis les agréger dans des rapports sur mesure afin de les représenter graphiquement.

Vous devez pouvoir mesurer vos progrès et efforts de remédiation grâce à une analyse des tendances en temps réel et générer des rapports d'analyse et de patch destinés à vos interlocuteurs. En effet, l'objectif n'est pas juste d'identifier les vulnérabilités et les actifs, mais plutôt de hiérarchiser ceux à remédier en premier.

CETTE ANALYSE MULTIDIMENSIONNELLE ET ITÉRATIVE DES DONNÉES VOUS PERMETTRA D'EXTRAIRE DES INDICATIONS ET DE CONNAÎTRE L'ÉTAT DE VOTRE SÉCURITÉ AUQUEL VOUS NE POURRIEZ SINON PAS AVOIR ACCÈS.





5

DES ÉVALUATIONS PRÉCISES DES SCÉNARIOS DE MENACES POUR VOTRE ENTREPRISE



Des évaluations précises du niveau de criticité de certains scénarios de menaces dans le contexte spécifique de votre entreprise pour détecter le risque avec précision



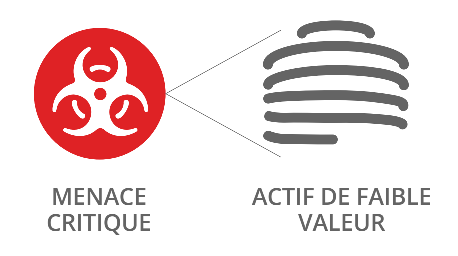
Vous pouvez enfin factoriser différents critères pour évaluer le niveau de criticité de certains scénarios de menaces dans le contexte spécifique de votre entreprise en vous appuyant sur des renseignements exploitables.

Après tout, chaque environnement IT est différent.

L'OBJECTIF : pouvoir hiérarchiser vos tâches de remédiation des vulnérabilités au sein d'un processus continu, contextuel, automatisé et précis.

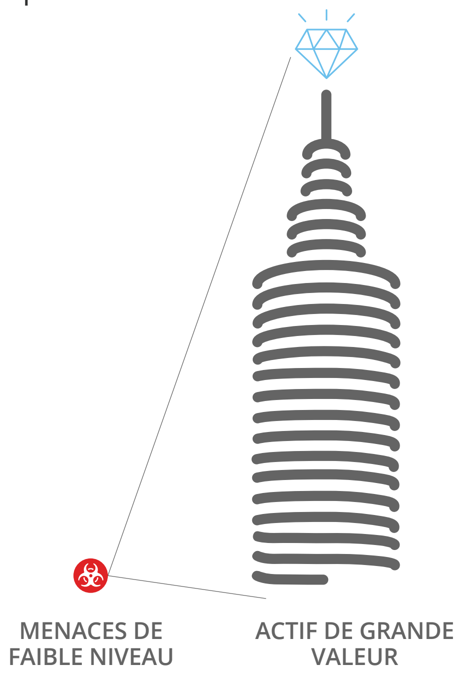
SCENARIO A :

Supposons qu'un logiciel de base de données vulnérable soit victime d'un exploit sauvage et en mode aveugle et sème le chaos dans de nombreuses entreprises. Votre entreprise est d'ailleurs peut-être concernée. Cependant, dans votre environnement, ce logiciel de base de données n'est installé que sur un système d'une importance toute relative et qui est isolé du reste de votre infrastructure. C'est vous qui déterminez si le niveau de risque d'un actif compromis est négligeable ou non pour votre entreprise.



SCENARIO B :

De même, vous pouvez être confronté au scénario contraire où une vulnérabilité qui n'attire pas nécessairement l'attention du marché peut s'avérer fatale pour votre entreprise.



Qualys **ThreatPROTECT**

Submergé par les vulnérabilités ?

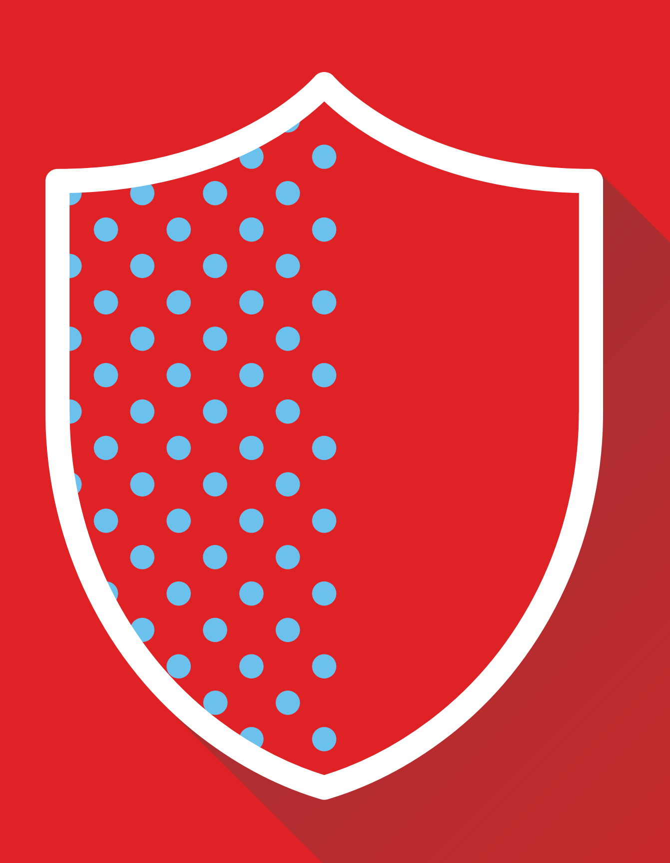
Qualys ThreatPROTECT vous permet de contrôler totalement les menaces en évolution permanente afin de connaître les vulnérabilités à remédier en premier.

De nouvelles vulnérabilités sont divulguées chaque jour, soit plusieurs milliers par an. Qualys ThreatPROTECT fait correspondre les renseignements sur les menaces actives avec vos données de vulnérabilités pour que vous puissiez détecter les actifs IT les plus à risque dans votre entreprise.

Grâce à ThreatPROTECT, vous disposez d'une vue globale holistique, contextuelle et actualisée en continu de votre exposition aux menaces. Dernier service ajouté à la plate-forme Qualys dans le Cloud, ThreatPROTECT vous évite de jouer aux devinettes et vous indique les vulnérabilités que vous devez remédier de suite.

ThreatPROTECT intègre un tableau de bord hautement personnalisable avec tout un éventail de modèles de rapports et de fonctionnalités de création de graphes. Ce service possède aussi un puissant moteur de recherche ainsi qu'un fil de renseignement en temps réel sur les menaces.

ThreatPROTECT affine la vision de votre équipe IT et lui fournit des renseignements exploitables via un processus de colmatage des failles de sécurité à la fois précis et stratégique



Qualys **ThreatPROTECT**

Identifiez les systèmes vulnérables grâce à une fonction de recherche de type Google.

Visualisez rapidement l'exposition de vos systèmes à des menaces actives telles que des Zero-Day, des vulnérabilités activement attaquées, etc.

Mesurez vos progrès et vos efforts de remédiation grâce à une analyse des tendances en temps réel.

Fil de renseignement en direct sur les menaces permettant aux ingénieurs en sécurité Qualys de valider et d'évaluer en permanence les nouvelles menaces issues de sources internes et externes.

Recevez une alerte dès que de nouvelles menaces actives surgissent dans votre environnement et lorsque les seuils définis par les utilisateurs sont atteints.

Pour demander une version d'évaluation gratuite de 14 jours, rendez-vous sur **qualys.com/ThreatPROTECT**

